Canvassing the Cyber Security Landscape: Why Energy Companies Need to Pay Attention

TUESDAY, 18 MAY 2010 00:00 BRUCE AVERILL AND ERIC A.M. LUIIJF

Recent news of a “highly sophisticated and targeted” cyber attack on Google, Yahoo, and perhaps on as many as a dozen other companies has once again brought the issue of cyber security to the top of the news. Internet companies, however, are not the only ones vulnerable to such attacks. Over the past decade, a series of events has highlighted the vulnerability of the electric grid and other energy infrastructures to both cyber disruptions (due, e.g., to malware) and from outside attacks using cyber methods.

Perhaps the most compelling examples have been the extensive blackouts in the Northeastern US and Western Europe during the late summer and early fall of 2003. They demonstrated in a convincing way the fragility of the energy infrastructure and the possibility of cascading failures due to problems with control system hardware and/or software. Over the same period of time, a series of highly publicized cyber attacks on structured queried language (SQL) servers (SQL is the language a computer uses to request information from a database) all over the world (Slammer, January 2003). Other attacks have included those directed against government sites (Estonia, April 2007; Georgia, August 2008; and the US, July 2009), and social networking sites (Facebook, August 2009; Twitter, August and December 2009), which demonstrated the ability of hackers and/or criminals to penetrate even well-guarded sites via the internet. Most recently, the US investigative television news program “60 Minutes” presented undocumented assertions that unspecified criminals or hackers have previously disrupted the power grid in Brazil, supporting earlier claims to that effect by the CIA regarding several unnamed countries.

Historical Background

For obvious reasons, to date no government, utility, or energy company has officially stated that a major power outage or similar event has been caused by a cyber attack. That being said, numerous reports have appeared attributing specific incidents to cyber attacks. Although reports from the CIA do not name specific countries, they do claim that in at least one case, multiple cities were affected, and that the attacks were subsequently followed by blackmail or extortion attempts. Perhaps the closest thing to a smoking gun is a series of power outages in Brazil in 2005, 2007, and 2009. Brazil has steadfastly denied that a cyber attack occurred in either 2007 or 2009, attributing the 2007 outage to “sooty insulators” on high-voltage lines. In contrast, a number of analysts believe that at least the 2005 event was due to Supervisory Control and Data Acquisition (SCADA) disruptions caused by hostile intrusion via the Internet.

Moreover, malware and hackers are known to have penetrated numerous times into critical supervision parts of the power grids in Australia, Europe, and the U.S. Examples include nuclear power plants being shut down due to cyber disruptions, near loss of control of a national control system in Australia due to malware, and a hacker who was able to wander around in a large European transmission system operator’s grid for 10 days.

Classified reports from around the globe indicate that main SCADA operator consoles of both refineries and large chemical plants have been penetrated by hackers for days. Similarly, malware has penetrated control systems on offshore oil and gas platforms a number of times, resulting in the risk of uncontrolled release of gas or oil and potential environmental damage, as well as possible explosions and loss of the platforms.

"Red Teams" of mock intruders from the Department of Energy’s four national laboratories have devised what one government document listed as "eight scenarios for a SCADA attack on an electrical power grid" -- and all of them worked. At least eighteen such exercises have been conducted against large regional utilities over the last several years. In 2002, Richard A. Clarke, President G. W. Bush's cyber security adviser, was quoted as saying that "the intruders … have always, always succeeded.” Subsequently, many more “Red Team” intrusions have been attempted, and all but one were successful. In the one unsuccessful attempt, the Red Team was forced to break off its penetration because hackers from a foreign nation were simultaneously penetrating along the same path.

Also relevant is evidence that a concerted cyber attack against Georgian government sites, including those used to control the Baku-Tbilisi-Ceyhan (BTC) pipeline, was an integral part of the Russian attack on Georgia in August 2008. Although the flow of oil and gas through the BTC and its parallel gas pipeline was never in fact disrupted—despite not only cyber attacks, but reported bombing attempts by Russian forces—the events can certainly be interpreted as sending a strong message about Russia's willingness and ability to use offensive cyber operations to achieve its goals.

Cyber attacks can also be used as a tool in information warfare. As an example, Russian hackers were apparently able to penetrate a nuclear power plant near St. Petersburg in May 2008. The website was taken offline at the same time as rumors of "radioactive emissions" from the plant were circulated, and for several hours there was apparently no effective communication between the plant and Rosatom, the state nuclear corporation. This intrusion did not affect operation of the plant, but it did open the door for potential panic among nearby residents (who could have, for example, overdosed on iodine to protect themselves against a non-existent radiation leak).

Evidence has been mounting over the past decade that cyber spies have routinely succeeded in penetrating the US electric grid, often leaving behind software that could, in theory, be used to disrupt the flow of electricity. Due to their sophistication, most such incidents to date have been attributed to Chinese and Russian operatives rather than to terrorist groups. Although most of these intrusions were detected by US intelligence agencies rather than by the companies that own and operate the infrastructures, company officials have clearly become aware of the problem. A 2008 survey of senior management and network engineers and administrators in a variety of industries revealed that more than half of them had already experienced a cyber intrusion, a leak of data, or an insider attack. Further, about one in seven were expecting a similar incident within the next year.

Key Vulnerabilities

By far the greatest point of concern in the industry is the vulnerability of industrial control systems, particularly the SCADA systems that are used to control dispersed physical assets or devices from a central location. Historically, SCADA systems antedate the development of the internet; they were originally hard-wired systems primarily intended to control processes at a single site and not designed to be connected to the outside world. However, with the advent of cheap PCs, improved telecommunications and the internet, these individual sites have become linked to one another and, in many cases, to the outside world via the internet. Moreover, the liberalization of the energy market requires energy production companies to continuously share their production and reserve capacity data with market operators and transmission system operators directly from their SCADA-controlled systems.

The United States, like most developed countries, depends upon three distinct grids to distribute energy from where it is generated to where it is consumed: the electric grid (which in the US is itself actually three electric grids: the Eastern, Western, and Texas Interconnects), a natural gas pipeline network, and a network of pipelines for distribution of petroleum and petroleum products. The flow of materials through all of these grids or networks is controlled via generators, switches, valves, compressors, odorizing stations, and pumps that utilize various types of SCADA devices and software.

Because most companies use the same computers and networks both to control internal operations and for business that requires contact with the outside world, the control systems are intrinsically vulnerable to any intruder who can penetrate a company's firewall (or to unintentional intrusions caused by unsafe browser settings or employee actions, such as neglecting to scan an attachment for viruses before opening). In addition, many systems have multiple wireless points of access that an intruder can exploit. Insider and third-party engineer access is also always a concern.

Most non-specific forms of malware will essentially shut down an operating system. Industrial control systems are even more sensitive to malware than your laptop. Of much more concern, however, is systematic exploitation of vulnerabilities by criminal or even terrorist organizations for financial or political gain. In particular, the high value of the commodities flowing through the grids or networks makes them very attractive targets for exploitation by criminal elements, either by means of fraudulent transfer of funds, rerouting of energy flows, or by extortion attempts. Indeed, the field abounds with unsubstantiated reports of companies and industries that have received threats to their service unless an appropriate fee is paid.

Although most attention is usually focused on threats to the electric grid, in practice there is no real difference in vulnerabilities between electric grids, natural gas pipelines, petroleum pipelines, district heating, and other utilities such as drinking water and sanitation systems. This point has been explicitly recognized by the American Gas Association, which has formulated specific recommendations for the gas industry to protect its SCADA communications from cyber attacks (AGA Report No. 12).

The Dutch document on SCADA security, "Good Practices for the Drinking Water Sector," is another case in point. The authors' files contain data on a large number of incidents that illustrate the adverse effects of process control weaknesses and vulnerabilities. In 2001, for example, installation of incorrect control software in one of the control computers in the gas mixing station in the municipality of Borssele in The Netherlands resulted in a malfunction that caused the utility's gas to contain such a high percentage of nitrogen that it would not burn. This led to a potentially hazardous situation that could have resulted in carbon monoxide poisoning, fires, or explosions. The situation was exacerbated by the failure of the central control room (some 37 kilometres away) to detect the non-standard gas blend for some time. As a result, some 26,000 households were without heat for about three days. Rectifying the situation required a massive effort by the police, fire brigades, and gas repair staff from across the entire country, since the nitrogen-rich mixture had to be removed from the gas on a street-by-street, house-by-house, and appliance-by-appliance basis.

The "Aurora effect", from the name of its US Department of Energy demonstration project, showed how cyber manipulation of the SCADA system of an electric generation plant could cause major physical damage to the plant's equipment, rather than just turning the electricity on or off. Video has been posted on the internet showing a multi-ton diesel generator shaking, smoking, throwing off parts of the machinery, and grinding to a halt in an experiment where investigators were able to access the generator remotely and vary its operating cycle in a particular way. Another example is a so-called "data storm", in which too much data in the control network blocks its ability to monitor and control the physical process. There is at least one documented example of a nuclear power plant in Alabama being shut down from this cause. In this case, a faulty control mechanism within the plant apparently generated so much data that it overwhelmed the device that controlled the plant's recirculation water pumps. Although this phenomenon occurred entirely within the plant, there is little reason to suppose that a similar effect could not be achieved remotely via the internet.

In 2008, a software update of a single office computer in the Baxley nuclear power plant in Georgia and its subsequent reboot caused the nuclear reactor to "scram." This constitutes yet another case where the control systems were not well separated from office systems and the public networks. Under normal circumstances, the decision to reduce costs by merging the office network with the SCADA process control network into a single physical network works flawlessly. If, however, this combination possesses a low bandwidth link between two locations, and the office network becomes overloaded due to malware, the control system network may slow down considerably. During the onset of the US 2003 blackout, this type of phenomenon resulted in loss of control of at least one regional power transmission system.

Key Threats

Cyber attacks are carried out by a variety of actors with different motivations, but it is convenient to consider four different categories. In order of increasing capability and threat, they are recreational, activist, criminal, and state-sponsored. Recreational hackers are largely motivated by the challenge of demonstrating their ability to hack into a protected server. The nature of the server (industrial vs. commercial vs. governmental) is often of secondary importance. Recreational hackers are often young and technically opportunistic, trolling many servers to locate one that they are able to penetrate. Because due diligence on the part of the system operator will keep them out (at least most of the time), they constitute by far the least serious threat to energy infrastructure.

In contrast, the other three types of hackers tend to target specific servers in order to advance a specific agenda. Activists (often referred to as "hacktivists") view cyber attacks as a tool that allows them to advance a particular political, social, or economic issue. For example, anti-nuclear or zero-hydrocarbon activists could try to disrupt the control system of a nuclear or fossil fuel facility in order to generate adverse publicity, illustrating the supposed dangers of relying upon either of these energy sources.

Criminals view cyber attacks as a tool that allows them to make money easily with minimal risk of apprehension. They tend to not be highly specific with regard to targets, but are highly opportunistic in exploiting perceived vulnerabilities that can generate revenue. In the energy sector, this could lead to manipulation of specific markets or to extortion by threatening to disrupt the electric grid unless a fee for "protection" is paid.

Finally, state actors have a variety of possible motivations, including commercial, military, tactical, and strategic. In many countries, the distinction between the public and private sector is not as well defined as in others, and cyber attacks can be used to install portals for automatic export of sensitive commercial data to further the business objectives of a nationally owned company. The potential use of such techniques to obtain sensitive military or government information to advance national interests is obvious. More importantly, however, state actors can also leave behind hidden re-entry gates that could be used as a tactical or strategic attack point in an international confrontation. Disrupting energy flows within a country could certainly create chaos, forcing the target nation to divert attention and manpower to dealing with internal issues rather than an external conflict.

Regardless of the identity of the attacker, however, by far the largest cyber security risk to energy infrastructure comes from the human components of the system, whose lack of security awareness is often aided and abetted by a lack of management vision and attention. Employees have been known to insert USB thumb drives of questionable origin into network computers (not realizing that they could have been pre-loaded with malware), bypass security controls in order to connect secure process control networks to the outside world, and allow third party engineers to connect contaminated laptops to the network. Moreover, the energy industry standard seems to be evolving to one that uses wireless modems or direct internet access to core control systems in order to facilitate third party maintenance as well as remote operation from home. Because of the convenience for operators, the resulting vulnerabilities and risk are often neglected. Hackers and malware build upon such weaknesses.

The top management of energy companies (generation, transport, distribution) that rely upon process control systems often neglect the risk of cyber disruption to these systems. Relatively few serious incidents have made the headlines, and consequently it is easy to assume that the risks are low or non-existent. Exacerbating the lack of awareness is the tendency of middle management to minimize the importance of evidence that unauthorized cyber access to their control networks has occurred in order to avoid embarrassment (or worse). Unfortunately, energy and other sectors that utilize process control systems lack a professional, worldwide incident-reporting mechanism. Without trying to assign blame or cast aspersions, it is high time for these sectors to collectively recognize the dangers and to learn how to prevent cyber disruptions. Energy systems are so critical to our societies that an approach similar to the incident-reporting system used by the international air transportation industry is urgently needed.

Most headlines that address cyber security issues focus on intrusions by international criminal or terrorist elements. In this regard, Chinese and Russian hackers have attracted the most attention. While it is intrinsically difficult to trace an attack back to its actual originator with any degree of certainty, a large amount of evidence has pointed to China and Russia as the source of many large-scale intrusions. The most potentially damaging attacker, however, is a technically competent insider,` more often than not a disgruntled employee or a person acting for political or ideological reasons. Normal security procedures mandate extensive screening of personnel with administrator-level access to control systems, and as a result very few such incidents have been reported. (It must be noted, however, that very few companies would find it in their best interests to publicize such incidents, unless they are required by law to do so.) One example of an insider attack is provided by the actions of an information communications technology (ICT) contractor for an oil and gas field developer, who, upon learning that he would not be offered a full-time position, reprogrammed the company's control system to disable its leak detection ability.

Future Risks

Energy markets can be manipulated by either rumors (often propagated via social networking sites) regarding, for example, an attack on and closure of a major gas or oil pipeline, or direct manipulation of spot market prices at power and gas exchanges such as Powernext, one of the European spot market energy exchanges. Such manipulations could lead to unexpected shortages in power or gas grids that cannot be resolved in time to avoid disruptions such as brownouts. This is not just a theoretical concern: over the past year or so, criminals have manipulated the European carbon credit market, with losses estimated at over 5 billion Euros.

The next big cyber security concern looming on the horizon is provided by the impending widespread implementation of smart grid technology, which is a critical component of 21st century energy systems. Smart grids will use digital technology to save energy, decrease costs, reduce emissions, and enhance system reliability. Unfortunately, however, increasing the digital connectivity of grids also increases the number of potential vulnerabilities. Indeed, the thought of millions of physically unprotected devices connected to the grid via the Internet sends collective shivers down the spines of cyber security professionals (especially if some of those homes also contain technologically sophisticated and intellectually curious teenagers.) In addition to

inadvertently causing massive disruptions of service, intruders could also arbitrarily turn off the power to thousands of homes or randomly charge users a higher rate than appropriate, while skimming the difference to their own account. Activists could find ways to switch grids on/off, make them appear unreliable, and cause financial loss to the grid operators in order to increase public awareness of their cause. It is therefore absolutely crucial that cyber security of smart devices is made a very high priority as smart grid technology becomes more and more ubiquitous.

The Road Ahead

The public and, more importantly, lawmakers and regulators are becoming increasingly better informed regarding the vulnerability of energy facilities and infrastructure to cyber disruptions and attack. A concerted and cooperative effort by academia, manufacturers, industry leaders, and policymakers is required to secure our energy systems (oil, gas, power, and district heating) against such disturbances. In the absence of firm and positive actions by the energy industry, national regulatory systems and international communities may prove to be too slow to respond to rapidly evolving threats. Above all, the top management of energy companies needs to be aware of the risk and take appropriate action. Rather than being neglected or downplayed, incidents need to be investigated and acted upon in a cooperative international fashion just as near misses and crashes are in the aviation industry.

One potentially useful approach would be to bring together CIOs (and possibly CEOs) from energy companies, government agencies, and network security providers to discuss details about actual incidents behind closed doors. The key is to convince participants that revealing weaknesses that they have overcome is an effective way to learn about potential threats before they happen. The goal would be to drive the creation of a cross-sector national plan to improve cyber security at each participating company or agency, thus strengthening the entire sector.

Additionally, national governments could prove to be a crucial source of threat information, good practices, and technical support for various industry players. Whatever methodology is eventually used, it is clear that it is in the best interests of the energy industry, governments, and, of course, consumers to take this threat seriously and to move expeditiously to confront it.

Dr. Bruce Averill is Founder and Senior Partner of Strategic Energy Security Solutions LLC; he was formerly Senior Coordinator for Critical Energy Infrastructure Protection Policy at the US Department of State. Eric A.M. Luiijf is Principal Consultant for Critical Infrastructure Protection at TNO Defence, Security and Safety (Netherlands Organisation for Applied Scientific Research).

Article from the Journal of Energy Security; May 2010